amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Carlo Rizzo

FASCICOLO N. 4/2024

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Francesco Cardarelli, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Chiara Cudia, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Bruno Mercurio, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Josè Manuel Ruano de la Fuente, Leonardo J. Sańchez-Mesa Martĭnez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Sveva Bocchini, Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Andrea Marco Colarusso, Sergio Contessa, Beatrice Coppa, Giuseppe Doria, Manuel Delgado Iribarren, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Giuseppina Lofaro, Federica Lombardi, Gaetano Natullo, Carmen Pérez González, Giovanni Pesce, Benedetta Piazza, Marcin Princ, Sara Pugliese, Bianca Nicla Romano, Antonio Saporito, Giuliano Taglianetti, Simona Terracciano, Stefania Terracciano, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Gli strumenti di AI nel piano nazionale per la digitalizzazione del patrimonio culturale. Prime osservazioni

di Luigi Ferrara

(Professore associato presso l'Università degli Studi di Napoli "Federico II")

Sommario

1. Premessa. L'introduzione degli strumenti di AI nei singoli settori dell'amministrazione italiana e nell'amministrazione del patrimonio culturale. – 2. Il regolamento UE 2024/1689 e l'ordinamento della cultura. – 3. Alcuni nodi problematici nel PND e nelle linee guida per la digitalizzazione del patrimonio culturale. – 4. Considerazioni conclusive. Le iniziative italiane di riforma legislativa ed il settore dei beni culturali.

Abstract

The article deals with the legal regulation of artificial intelligence tools in the cultural heritage system, currently being defined following the adoption by the MIC in 2022 of the National Plan for the Digitalisation of Cultural Heritage (PND) 2022-2026. The contribution starts from some general issues regarding the introduction of AI in individual sectors of the Italian administration, to then analyse the evolution of the European legal framework following the entry into force of EU Regulation 2024/1689 on AI. The contents of the four "guidelines" for the digitalisation of cultural heritage attached to the PND and the ministerial organisational structure IPAC, Infrastructure for digital services related to the digitalisation of cultural heritage, which will have to provide the coordinates and specific digital AI services to the various cultural institutions, are then analysed. Finally, the ongoing national legislative initiatives for the overall regulation of AI tools are analysed.

* *Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review*

ISSN 2036-7821

1. Premessa. L'introduzione degli strumenti di AI nei singoli settori dell'amministrazione italiana e nell'amministrazione del patrimonio culturale.

Nel corso degli ultimi due anni, in attuazione delle riforme previste dal PNRR, anche nel nostro ordinamento settoriale dei beni e delle politiche culturali è possibile osservare l'introduzione di alcune fonti di disciplina giuridica degli strumenti di intelligenza artificiale da parte delle istituzioni culturali pubbliche e private. Il presente contributo si propone di analizzare, in particolare, alcune questioni giuridiche emergenti a seguito dell'adozione da parte del MIC nel 2022 del Piano nazionale per la digitalizzazione del patrimonio culturale (PND) 2022-2026.

Le istituzioni culturali italiane (quelle museali in particolare) sono, da un lato, destinatarie delle previsioni del piano nazionale, ed in particolare delle *linee guida allegate* al piano, dall'altro sperimentatrici già da alcuni anni di autonome iniziative di uso dell'intelligenza artificiale nella gestione del patrimonio, nei servizi e nelle attività museali, mutuando spesso le esperienze maturate da molte istituzioni museali straniere e collaborando con esse, in ordine alle quali occorre individuare una tassonomia, in un quadro giuridico incerto, che solo faticosamente potrà essere ricondotto a unità dalle iniziative legislative e di inquadramento generale in atto, di cui si terrà conto nella parte finale di queste brevi riflessioni[1]. La riflessione non può che muovere da alcune tematiche generali in tema di introduzione dell'AI nei singoli settori dell'amministrazione italiana, per analizzare poi l'evoluzione del quadro giuridico europeo a seguito dell'entrata in vigore del Regolamento UE 2024/1689 sull'AI. Vengono quindi analizzati i contenuti delle quattro "linee guida" per la digitalizzazione del patrimonio culturale allegate al PND e la struttura organizzativa ministeriale "IPAC", *Infrastruttura per i servizi digitali legati alla digitalizzazione del patrimonio culturale*, che dovrà fornire le coordinate e gli specifici servizi digitali di IA alle diverse istituzioni culturali. Infine, sono oggetto di analisi le iniziative legislative nazionali in atto di disciplina complessiva degli strumenti di AI.

L'analisi della letteratura e degli orientamenti giurisprudenziali più recenti sull'uso degli strumenti di AI da parte delle pubbliche amministrazioni, evidenzia che, quando la dottrina giuridica approccia i temi dell'intelligenza artificiale - sia che si muova nella

[1] La letteratura sull'introduzione di strumenti di intelligenza artificiale da parte di istituzioni culturali non è ancora amplissima. *Ex multis*, cfr. L. PAPI, A. PETRILLO, *L'intelligenza artificiale applicata al patrimonio culturale: Una innovazione tecnologica per la conservazione e la valorizzazione del patrimomio culturale* , in *Archeomatica*, *14*(2), 2023; G. DI MARCANTONIO, *Intelligenza artificiale, Large Language Models (LLMs) e Retrieval-Augmented Generation (RAG). Nuovi strumenti per l'accesso alle risorse archivistiche e bibliografiche*, in *Bibliothecae.it*, 13(1), 2024, 146-173; C. GRECO, C. ROSSI, S. DELLA TORRE, *Digitalizzazione e patrimonio culturale tra crisi e opportunità: l'esperienza del Museo Egizio di Torino*,in *Il capitale culturale*, Supplementi 11, 2020, 197-212; O. MURPHY, E. VILLAESPESA, *Musei e intelligenza artificiale*, IULMaiLAB, 2024; D.H.R. SPENNEMANN, *Will Artificial Intelligence Affect How Cultural Heritage Will Be Managed in the Future? Responses Generated by Four genAI Models*, in *Heritage*, 7, 2024, 1453–1471; P. NIKOLAOU, *Museums and the Post-Digital: Revisiting Challenges in the Digital Transformation of Museums*, in *Heritage*, 7, 2024, 1784–1800; J WEN, B. MA, *Enhancing museum experience through deep learning and multimedia technology*, in *Heliyon*, 10(12), 2024;

ISSN 2036-7821

prospettiva dell'ordinamento generale sia che approfondisca ordinamenti settoriali - prediliga, alternativamente o congiuntamente, tre punti di vista: quello delle situazioni giuridiche soggettive e della loro tutela, quello del procedimento e della decisione algoritmica come risultato di esso, ovvero quello organizzativo, e quindi il tema dell'infrastruttura digitale necessaria, la sua realizzazione, utilizzazione e manutenzione, i profili proprietari e i rapporti di partenariato con le imprese digitali. In questo contributo, come si evidenzierà meglio in seguito, quest'ultimo sembra l'approccio che maggiormente consenta di far emergere i profili critici del PND.
Come si vedrà meglio nel paragrafo successivo, a seguito dell'entrata in vigore del Regolamento Europeo n. 1689 del 2024, anche nell'organizzazione delle attività e dei servizi delle pubbliche amministrazioni attraverso strumenti di AI si afferma la necessità dell' "approccio del rischio", declinato anche come approccio del rischio rispetto all'organizzazione e, quindi, all'infrastruttura. Occorre quindi interrogarsi se questo approccio del rischio sia adeguatamente presente nella disciplina in via di definizione dell'IA nel settore della cultura: se il PND e le sue linee guida dettino indicazioni operative per la struttura ministeriale, da un lato, e per le istituzioni culturali pubbliche e private (museali in particolare), dall'altro, coerenti con le regole e gli strumenti di prevenzione del rischio del Regolamento europeo. Ma, in prospettiva più ampia, occorre sottoporre al vaglio il PND e le linee guida anche in relazione alle evoluzioni della giurisprudenza più recente e alle altre discipline settoriali dell'AI introdotte negli anni più recenti. Innanzitutto, le indicazioni del Garante per la protezione dei dati personali, sulle implicazioni in tema di *privacy* degli strumenti di AI, ma anche la disciplina giuridica della dell'AI nei contratti pubblici, introdotta dal nuovo Codice dei contratti pubblici, D.Lgs. n. 36 del 2023, e infine quella del cd. *cybersicurezza*, rafforzata con la nascita dell'Autorità nazionale.

2. Il Regolamento UE 2024/1689 e l'ordinamento della cultura.

Come è noto il cd. *AI* Act, il Regolamento (UE) 2024/1689, dopo una lunga gestazione, è stato pubblicato sulla Gazzetta Ufficiale UE del 12.luglio 2024 ed diventerà integralmente efficace 24 mesi dopo la sua pubblicazione, a seguito della previsione di parti della disciplina ad efficacia variamente anticipata o differita (i divieti relativi a pratiche vietate; i codici di buone pratiche; le norme sui sistemi di IA per finalità generali; gli obblighi per i sistemi ad alto rischio). Il Regolamento, nei Considerando 1 e 6 e nell'art.1, definisce le sue finalità nella creazione di un quadro giuridico uniforme per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di "sistemi di intelligenza artificiale "*antropocentrica e affidabile*, protezione della salute, della sicurezza e dei diritti fondamentali. In particolare, nel Considerando 7, proprio per la necessità di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, viene sottolineata ancora la

ISSN 2036-7821

necessità di "*stabilire regole comuni per i sistemi di IA ad alto rischio*", coerenti con la CEDU, non discriminatorie e in linea con gli impegni commerciali internazionali. Sulla collocazione del Regolamento nel quadro delle fonti europee, il Considerando 9 definisce le regole introdotte dal Regolamento come *complementari* al quadro giuridico vigente, "*in particolare in materia di protezione dei dati, tutela dei consumatori, diritti fondamentali, occupazione e protezione dei lavoratori e sicurezza dei prodotti*", restando impregiudicati e pienamente applicabili tutti i *mezzi di ricorso* vigenti, rispetto ai quali il regolamento definisce ulteriormente "*requisiti e obblighi specifici, anche per quanto riguarda la trasparenza, la documentazione tecnica e la conservazione delle registrazioni dei sistemi di IA*". In particolare, come richiamato dal Considerando 157, restano impregiudicati "*le competenze, i compiti, i poteri e l'indipendenza delle autorità o degli organismi pubblici nazionali competenti che controllano l'applicazione del diritto dell'Unione che tutela i diritti fondamentali, compresi gli organismi per la parità e le autorità per la protezione dei dati.*" Nei Considerando 12-19, e più esaustivamente nell'art. 1, sono introdotte le definizioni fondamentali di "sistemi di AI", "deployer", "dati biometrici", identificazione e categorizzazione biometrica, "sistemi di riconoscimento delle emozioni", "spazio accessibile al pubblico", . Ai sensi dell'art. 3, i sistemi di IA sono definiti come sistemi automatizzati basati su macchine *per funzionare con diversi livelli di autonomia,* che possono avere *capacità di adattamento dopo l'installazione* e che, per obiettivi espliciti o impliciti, sono in grado di dedurre dagli input ricevuti e "*generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*", distinguendosi quindi dai sistemi software tradizionali per eseguire operazioni in modo automatico, come sottolineato nel Considerando 10. L'art. 2 introduce i settori esclusi dal campo di applicazione del Regolamento, tra cui i sistemi utilizzati per scopi militari, di difesa e di sicurezza nazionale - su cui restano impregiudicate le competenze nazionali - e di ricerca e sviluppo scientifico.

Come anticipato, ai sensi dell'art. 5 vengono definiti e vietati i sistemi di IA che rappresentano un *rischio inaccettabile* per i diritti fondamentali dei cittadini. In particolare, si tratta dei sistemi che: distorcono il comportamento attraverso tecniche subliminali o sfruttando vulnerabilità specifiche (dovute ad età, disabilità, etc.), in modo da causare o suscettibili di causare danni fisici o psicologici; consentono la valutazione e classificazione dell'affidabilità di persone fisiche mediante l'attribuzione di un "*punteggio sociale*" con finalità generali da parte di autorità pubbliche, tali da determinare trattamenti pregiudizievoli e o sfavorevoli; consentono l'*identificazione biometrica "remota"*, anche "in tempo reale" salvo casi eccezionali autorizzati dalla legge riconducibili ad attività di prevenzione e contrasto del crimine e soggetti a garanzie specifiche per il rispetto dei diritti fondamentali, come per la protezione delle vittime di reato e previa autorizzazione rilasciata da autorità amministrativa o giurisdizionale. Gli artt. 6-27, il cuore del Regolamento, definiscono poi i sistemi ad *alto*

ISSN 2036-7821

rischio, in quanto he potrebbero arrecare danni significativi alla salute, alla sicurezza, ai diritti fondamentali, all'ambiente riportati nell'Allegato III. Rientrano in questa categoria i sistemi legati alle infrastrutture critiche, istruzione e formazione professionale, occupazione, servizi pubblici e privati di base assistenza sanitaria, sistemi di contrasto e gestione delle migrazioni, sistemi legati all'amministrazione della giustizia e ai processi democratici. Per questi sistemi sono previsti obblighi rigorosi prima di essere immessi sul mercato, in modo che sia garantita la sicurezza e la trasparenza, la sorveglianza umana, la cybersicurezza, obblighi di informazione per il pubblico e di cooperazione con le autorità competenti, specifici sistemi di gestione dei rischi, tracciabilità dei risultati, etc., e obblighi di monitoraggio post implementazione, di condivisione di informazione su incidenti gravi, che consentano di elaborare una *banca dati* comune dei sistemi ad alto rischio, prevista dall'art. 71.
A partire dall'art. 50, sono poi individuati i sistemi a rischio limitato, e, più esattamente i sistemi *per finalità generali con rischio sistemico*. per i quali sono introdotti specifici obblighi di trasparenza, di introduzione di codici di comportamento, di valutazione dei rischi, di trasmissione di documenti alle autorità competenti, etc.
Le successive disposizioni del Regolamento definiscono gli *obbligo di formazione*, e, a partire dagli artt. 64ss., il sistema di *governance*, che prevede l'istituzione di un *Ufficio per l'IA*, presso la Commissione, e un *Consiglio per l'IA*, composto da un rappresentante per Stato membro, al quale partecipa anche il Garante europeo per la protezione dei dati, un *Forum consultivo* di *stakeholders*, a cui partecipano anche L'Agenzia per i diritti fondamentali, l'ENISA, il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto europeo per le norme di telecomunicazione (ETSI). Viene poi prevista l'istituzione di un *Gruppo di esperti scientifici indipendenti* selezionati dalla Commissione, per sostenere il lavoro dell'Ufficio per l'IA, delle autorità di vigilanza e degli Stati membri. L'art. 70 si occupa poi delle *Autorità nazionali competenti*, che ciascuno Stato deve istituire o individuare con compiti di vigilanza, che operino in modo indipendente e imparziale per garantire l'applicazione del Regolamento.
Gli artt. 79-82 definiscono le *procedure nazionali* e presso la Commissione di indagine sui sistemi di IA che presentino rischi e gli eventuali provvedimento conclusivi inibitori o sanzionatori. Gli artt. 85-94 definiscono le regole generali sui *mezzi di ricorso*, il diritto al contraddittorio, i poteri di indagine, monitoraggio, richiesta di informazioni ed esecuzione attraverso mi sure di da parte degli organismi di governance europei nei confronti dei *deployers* dei sistemi di AI a rischio sistemico. Gli artt. 99-101 definiscono il sistema delle sanzioni, che devono essere *effettive, proporzionate e dissuasive* e possono includere anche avvertimenti e misure pecuniarie e non pecuniarie e possono essere inflitte, oltre che degli organismi nazionali, dagli

ISSN 2036-7821

organismi della Commissione e dal Garante europeo dei dati personali, e possono poi essere oggetto di ricorso alla Corte di Giustizia.
Come si è visto, l'approccio del rischio definisce molto divieti ed obblighi per i *deployers* e poteri della autorità europee e nazionali. Ai fini della presente indagine occorre sottolineare quali disposizioni possano riguardare il settore della cultura e le istituzioni culturali. Innanzitutto, occorre sottolineare che la cultura è uno dei settori in cui possono essere implementati sistemi di AI oggetto del Regolamento, come richiamato dal Considerando 4. Inoltre, la *diversità culturale*, vien richiamata dal Considerando 27 come portato del principio di "*diversità, non discriminazione ed equità*", uno dei sette *principi etici* non vincolanti per l'AI elaborati dalla Commissione nel 2019. Più specificamente, poi, le attività e i servizi implementati dalle istituzioni culturali, di cui si è dato una sintetica rassegna nel paragrafo precedente, possono rientrare tra le attività *ad alto rischio* (ad esempio, i sistemi biometrici) o a medio rischio o *per finalità generali con rischio sistemico*. In tal caso, occorre verificare se le istituzioni nazionali, nel quadro vigente delineato dal PND, siano adeguatamente sollecitate all'applicazione del nuovo quadro di regole europee e dotate degli strumenti necessari.

3. Alcuni nodi problematici nel PND e nelle linee guida per la digitalizzazione del patrimonio culturale.

In materia di politiche culturali, il PNRR prevede la nascita di una Direzione generale per la digitalizzazione dei beni culturali, la Digital Library, e che ha approvato e ha avviato il piano per la digitalizzazione del patrimonio culturale. Una struttura organizzativa è stata istituita ed è in via di definizione operativa, la cosiddetta IPAC, infrastruttura per i servizi digitali legati alla digitalizzazione del patrimonio culturale, che dovrà fornire le coordinate e gli specifici servizi digitali di IA alle diverse istituzioni culturali, soprattutto le istituzioni museali pubbliche. Come premesso, il piano nazionale per la digitalizzazione del patrimonio culturale, poi, si struttura in quattro linee guida: una sulle tecniche di digitalizzazione; una sull'elaborazione del piano di gestione dei dati, una l'acquisizione, la circolazione e il riuso delle riproduzioni dei beni culturali in ambiente digitale, una sui servizi digitali e una sulla valutazione della maturità digitale degli istituti di cultura. Io credo, in estrema sintesi, che sia il piano sia le linee guida, sia l'infrastruttura in via di implementazione da parte di IPAC e Digital Library attraverso i cinque bandi per l'individuazione di partners privati finora adottati, sia le regole sull'implementazione di attività e servizi museali basati su algoritmi da parte delle istituzioni museali, non siano coerenti con l' approccio del rischio, ad esempio in ordine alla prevenzione e gestione dei bias nell'apprendimento o in ordine all'analisi preventiva di impatto, che sono richiesti dal regolamento europeo e, tra poco, anche dalla Convenzione. Ove il piano nazionale e le linee guida, soprattutto quelle contenute nell'allegato tecnico n.4, relative ai prodotti

ISSN 2036-7821

e servizi digitali, definiscono il ruolo della infrastruttura, a fronte di una apprezzabile prima tassonomia di questi prodotti e servizi (I servizi sono distinti in quattro categorie: servizi di gestione, servizi digitali di consumo, servizi digitali per la creazione di nuovi contenuti e servizi digitali a valore aggiunto), molto lacunosa appare: 1)l'indicazione delle modalità operative dell'infrastruttura; 2)le regole generali sui bandi; 3) quelle sui rapporti contrattuali con i privati, sia server hosts che software houses; 4) le relazioni organizzative tra Digital Library e IPAC in funzione di providers e istituzioni museali in funzione di deployers di attività, prodotti e servizi culturali basati su sistemi di AI; 5) Gli standard minimi di qualità di questi servizi digitali; 6) In tema dei bias cognitivi, appena accennati nella seconda tra le linee guida, relativa alla redazione dei piani per la gestione dei dati e assenti invece nelle altre linee guida, in particolare quelle sulla valutazione della maturità digitale, ovvero le procedure di controllo (che valutano la "maturità" delle istituzioni culturali esclusivamente con riferimento alla percentuale di utenti fruitori). Manca un riferimento alla necessità di una classificazione dei servizi sulla base del rischio, e la connessione della maturità digitale delle istituzioni culturali con l'implementazione di tecniche di governo del rischio, basate sull'elaborazione di esaustive valutazioni d'impatto.

Di cosa stiamo parlando specificamente?

Le linee guida per la classificazione di prodotti e servizi digitali, processi e modelli di gestione contenute nell'allegato tecnico n. 4 al PND, identificano quattro processi-tipo: 1) I luoghi della cultura mettono a disposizione degli utenti contenuti digitali per la consultazione e la navigazione;2) I luoghi della cultura mettono a disposizione contenuti digitali per creare ulteriori contenuti, scientifici o creativi, da parte degli utenti;3) I luoghi della cultura e/o gli utenti utilizzano i contenuti digitali e li rielaborano con un valore aggiunto per finalità espositive, educative, editoriali o commerciali; 4) I luoghi della cultura offrono esperienze di visita agli utenti, sia nella dimensione fisica che digitale.

A questi processi corrisponde la classificazione, come anticipato, dei prodotti i servizi in: servizi di gestione, servizi digitali di consumo, servizi digitali per la creazione di nuovi contenuti e servizi (e prodotti) digitali a valore aggiunto.

In particolare, nella quarta tipologia di processi (quelli legati alla visita reale o virtuale, cd. User journey) sono contemplate attività a rischio di profilazione, come controllo sicurezza, antifurto, capienza per sala, tracciamento dei flussi degli utenti, gestione emergenze, fidelizzazione degli utenti e la gestione delle attività post-visita.

Tra i processi post-visita, sono esplicitamente contemplati, tra gli altri, i servizi *analytics* di profilazione attraverso AI: offerta di contenuti che ripropongono l'esperienza; offerta di suggerimenti di approfondimento dei contenuti, di acquisto di attività e di servizi extra; abilitazione dell'utente all'interazione con i contenuti (cd. *user generated content*); abilitazione alla pubblicazione di feedback utente; offerta di

ISSN 2036-7821

suggerimenti d'acquisto/prestito; offerta di scontistica su acquisti; gestione dei prestiti e analisi di prestiti e acquisti effettuati; analisi delle preferenze e delle abitudini per target; analisi dei tempi di visita e consultazione degli utenti; coinvolgimento nelle attività dell'istituzione culturale (fund raising, crowdfunding); analisi dei contenuti fruiti e consultati dagli utenti (per mezzo dell'intelligenza artificiale è possibile analizzare le preferenze e gli interessi dei visitatori di un luogo della cultura, confrontarli con comportamenti passati di turisti e fornire raccomandazioni, orientamenti e indicazioni personalizzate); analisi dell'engagement sui social media; assistenza all'utente e reclami; offerta di membership o abbonamento.

Riguardo a tutti questi prodotti e servizi, che spesso contemplano, come si è visto, attività *analytics* di profilazione, nelle linee guida contenute nell'allegato 4 sono analizzati alcuni modelli di esternalizzazione e di internalizzazione dell'infrastruttura e dei servizi. Sono così individuate quattro tipologie: Gestione internalizzata con prodotti tecnologici custom; Gestione esternalizzata con prodotti tecnologici di mercato; Gestione esternalizzata attraverso acquisto di servizi SaaS; Gestione mista attraverso accordi di partenariato pubblico-privato.

I soggetti privati sono configurati come: 1) meri fornitori di servizi (operatori di mercato), che realizzano una progettualità che rimane nel dominio dell'istituto della cultura, che avrà quindi anche l'onere della gestione del servizio in esercizio; 2) partner che co-progettano e co-realizzano i prodotti o servizi (tipicamente i concessionari di servizi) a cui spetta in genere anche la gestione del servizio in esercizio; 3) soggetti "terzi" (tipicamente il terzo settore o le industrie culturali e creative) che realizzano prodotti e servizi per finalità non riconducibili alla missione dell'istituto. In tal caso i processi "*saranno quelli dell'operatore che eroga il servizio stesso, mentre all'istituto culturale spetterà la definizione di adeguate forme di accordo o concessione per l'utilizzo dei contenuti (modello royalty-based)*".

Non c'è nessun riferimento specifico alle cautele particolari nel senso di approccio del rischio in ordine all'infrastruttura, agli algoritmi, ai dati sensibili. Ma c'è invece uno stimolo a preferire esternalizzazione molto spinte, giustificate perché laddove un'istituzione culturale pubblica preferisse server interni, tecniche di archiviazione, di manutenzione, migrazione e gestione dati interne rischierebbe di andare incontro all'obsolescenza in pochi anni in assenza di risorse per la continua reingegnerizzazione dei sistemi, mentre invece affidarsi a un grande fornitore privato, si trova scritto, evidentemente riuscirebbe a scongiurare questa obsolescenza. Ecco, l'obsolescenza è l'unico criterio individuato all'interno delle linee guida in ordine alla preferenza per l'uno o per l'altro sistema.

Ma, come si è visto, non viene sviluppato un approccio del rischio coerente con il regolamento n. 1689 del 2024. Inoltre, le linee guida non chiariscono il framework normativo per i modelli di esternalizzazione o partenariato. Colpisce che delle linee

ISSN 2036-7821

guida tecniche non menzionino gli strumenti contemplati dal codice dei contratti pubblici, in particolare le norme in tema di contratti nel settore dei beni culturali, così da analizzarne il portato in questi servizi specifici. Colpisce ancora, nell'allegato 4 sui servizi più volte menzionato, l'assenza di rinvii alla disciplina europea e nazionale in tema di privacy.

4. Considerazioni conclusive. Le iniziative italiane di riforma legislativa ed il settore dei beni culturali.

In concomitanza con il lungo procedimento che ha portato all'approvazione del nuovo Regolamento europeo, il quadro legislative nazionale generale sull'AI inizia a delinearsi dapprima con alcune fonti di *soft law*, poi con la presentazione di un ddl in materia di AI. Il Consiglio dei ministri nell'aprile 2024 ha deliberato il disegno di legge "*Disposizioni e delega al Governo in materia di intelligenza artificiale*", presentato in Senato il 20 maggio 2024, A.S. 1146. Il testo è suddiviso in sei Capi e costituito da 26 articoli, e disciplina l'uso dell'IA con riferimento a diversi settori: sanità (art. 7-9), lavoro (art. 10-11), professioni intellettuali (art. 12), pubblica amministrazione (art. 13), attività giudiziaria (art. 14), cybersicurezza (art. 16). Inoltre, nell'ambito della strategia nazionale sull'IA e delle azioni di promozione (art 17-22), il disegno di legge prevede investimenti (art. 21), la tutela del diritto d'autore con riguardo alle opere generate con l'ausilio dell'IA (art. 24), e alcune modifiche al codice di procedura civile (art. 15) e penale (art. 25). L'articolo 2, alla lettera *a)*, reca la definizione di sistema di intelligenza artificiale. Con tale termine si intende un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che puo` presentare adattabilita` dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. La lettera *b)* introduce la definizione di dato, considerato come qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva. Infine, la lettera *c)* riporta la definizione di modelli di intelligenza artificiale. Si tratta di modelli che identificano strutture ricorrenti attraverso l'uso di collezioni di dati, che hanno la capacita` di svolgere un'ampia gamma di compiti distinti e che possono essere integrati in una varietà di sistemi o applicazioni. L'articolo 3 definisce i principi generali della disciplina: il rispetto dei diritti fondamentali e delle liberta` previsti dall'ordinamento italiano ed europeo; i principi di trasparenza, proporzionalita`, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parita` dei sessi e sostenibilita`; correttezza, attendibilita`, sicurezza, qualita`, appropriatezza e trasparenza, secondo il principio di proporzionalita`, dei dati e processi su cui si sviluppa l'intelligenza artificiale; il rispetto dell'autonomia e del potere decisionale umani; la prevenzione

ISSN 2036-7821

del danno; la conoscibilita` e spiegabilita`. L'utilizzo di sistemi di intelligenza artificiale non deve recare pregiudizio allo svolgimento con metodo democratico della vita istituzionale e politica. Vien poi richiamata la cybersicurezza (protezione dagli attacchi informatici) lungo l'intero ciclo di vita dei sistemi e modelli di intelligenza artificiale, sulla base del rischio e con specifici controlli di sicurezza, con riguardo tra l'altro ai tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza. Infine, il comma 6 richiama l'accesso delle persone con disabilita` su base di uguaglianza e senza alcuna forma di discriminazione e di pregiudizio. L'articolo 4 reca principi specifici, in materia di informazione e di riservatezza dei dati personali. Una specifica disposizione ha ad oggetto l'accesso dei **minori** alle tecnologie di intelligenza artificiale. L'art. 5 introduce poi i principi in tema di sviluppo economico, disponendo innanzitutto che le autorità pubbliche debbano promuovere l'utilizzo dell'AI facilitando la disponibilità di dati di alta qualità e favoriscano la creazione di un mercato dell'intelligenza artificiale innovativo, equo, aperto e concorrenziale, indirizzino le piattaforme di *e-procurement* delle amministrazioni pubbliche, garantiscono la localizzazione e l'elaborazione dei dati critici presso *data center* posti sul territorio nazionale. L'articolo 6 esclude dall'ambito applicativo della disciplina prevista le attività connesse ai sistemi e modelli di intelligenza artificiale, condotte dagli organismi preposti alla sicurezza nazionale, alla cybersicurezza, alla difesa nazionale. Rimangono fermi peraltro alcuni loro obblighi, anche in materia di trattamento dei dati personali. Una più analitica disciplina di rango applicativo e` demandata a successivi d.P.C.M. L'articolo 7 enuncia alcuni principi volti a regolare l'uso dei sistemi di intelligenza artificiale in ambito sanitario, con particolare riguardo al miglioramento delle condizioni di vita delle persone con disabilita`, stabilendo il divieto di condizionare l'accesso alle prestazioni sanitarie a criteri discriminatori, e riaffermando la necessaria garanzia della protezione dei dati sensibili e il diritto di informazione.

In materia di attività culturali, l'art. 23 del disegno di legge e reca disposizioni a tutela degli utenti e in materia di **diritto d'autore,** introducendo procedure per consentire agli utenti di riconoscere i contenuti generati da IA. Vengono dettati i principi in materia di informazione nel settore dei servizi media audiovisivi e radiofonici e stabilito, in particolare, che la disciplina dell'informazione radiotelevisiva debba garantire, tra l'altro, il divieto di utilizzare metodologie e tecniche capaci di manipolare in maniera non riconoscibile allo spettatore il contenuto delle informazioni, mettendo al corrente dell'alterazione o creazione di contenuti informativi anche quando questo avvenga attraverso l'utilizzo di sistemi di intelligenza artificiale. La disposizione prevede poi l'obbligo dei fornitori di piattaforme per la condivisione di *video* soggetti alla giurisdizione italiana di adottare misure adeguate volte a tutelare i minori e il grande pubblico da taluni programmi o

ISSN 2036-7821

video considerati lesivi per la persona. La novella estende tale obbligo, prevedendo che le suddette misure debbano essere adottate anche al fine di tutelare il grande pubblico da contenuti informativi che siano stati, attraverso l'utilizzo di sistemi di intelligenza artificiale, completamente generati ovvero, anche parzialmente, modificati o alterati in modo da presentare come reali dati, fatti e informazioni che non lo sono. L'**articolo 24** disciplina la **tutela del diritto d'autore** con riguardo alle opere generate con l'ausilio dell'**intelligenza artificiale**. In particolare, tramite novelle alla legge sul diritto d'autore, si precisa che le "opere dell'ingegno" protette devono essere di **origine "umana"** e, in secondo luogo, che **anche le opere create con l'ausilio di strumenti di intelligenza artificiale** sono protette dal diritto d'autore, a condizione che la loro creazione derivi del lavoro intellettuale dell'autore.
Viene inoltre consentita la **riproduzione** e **l'estrazione**, effettuata **tramite l'utilizzo di modelli e sistemi di intelligenza artificiale**, compresi quelli generativi, **di opere o altri materiali**, in conformità alla disciplina del diritto d'autore.
Come si può osservare, anche il ddl non introduce principi generali specifici per il settore della cultura e del patrimonio culturale, ad eccezione delle disposizioni da ultime contemplate. Restano quindi ferme le perplessità sottolineate, in attesa dei successivi sviluppi attesi, con l'approvazione del ddl, l'adozione dei decreti legislativi e, si auspica, la revisione/integrazione delle linee guida allegate al PND.

ISSN 2036-7821